戦略的国際科学技術協力推進事業日本－フランス(CNRS)研究交流
平成 22 年度終了課題事後評価報告書

1．研究課題名：「暗号と理論：計算機によって検証された安全性証明

2．研究代表者名：

2－1．日本側研究代表者：**産業技術総合研究所　情報セキュリティー研究センター**
研究センター長　今井　秀樹

2－2．フランス側研究代表者：**CNRS, Ecole Normale Superieure de Cachan and INRIA　教授**
Jean GOUBAULT-LARRECQ

3．総合評価：（　優　）

4．事後評価結果

（1）研究成果の評価について

本共同研究は、ネットワーク社会における電子的なデータのやりとりの安全性に関して、日本側の暗号理論に基づくセキュリティ技術とフランス側の論理学に基づく計算機技術を組み合わせて、記号レベルで安全性の証明を行うことを目的に、計算量理論的に健全な形式的安全証明と計算機を用いた暗号技術の形式的安全証明の課題について、理論構築と技術開発を行ったものである。その結果として、厳密な計算量理論的安全性検証のための枠組みを与えたこと、 セキュリティプロトコルが計算機上で複数セッション同時に実行されている状況でのプロトコルの安全性検証法を提案したこと、セキュリティプロトコルに用いられる疑似乱数発生器のソフトウェア実装の安全性を検証する方法を示したこと、などの成果を挙げた。これらの研究成果は多くの共著論文にまとめられており、日仏研究交流による相乗効果が認められる。

研究成果はかなり専門的であるので、その効果や社会的なインパクトを一般の人にも分かり易く説明することが望まれる。これらの成果を現実のシステムへ応用する場合の実際の安全性の検証・評価に向けて今後も一層の研究推進が望まれる。

（2）交流成果の評価について

本事業の趣旨に合致した密接な研究交流が行われ、多くの研究者が集ってワークショップを中心に交流を深めることにより、成果をあげることができたことは評価できる。H. Comon-Lundh 教授が日仏双方に所属したことが緊密で継続的かつ実質の伴った連携に役立ち、日本側の暗号学研究者と仏側の論理学研究者の相補的な研究協力が実現したと認められる。 日、仏で行われたスプリングスクール形式のオープンなワークショップは盛況でレベ

ルが高く、この分野の世界的な研究に貢献した。

本共同研究は、安全性証明に対する暗号学的アプローチと論理学的アプローチのギャップが注目され、2つのアプローチの融合が求められている時期に、非常にタイムリーな研究交流であった。情報セキュリティは社会的にますます重要度を増している課題である。困難も伴うが、情報社会の安全性確保のために必要な基礎研究なので、今後の更なる展開を期待する。

(3)その他(研究体制、成果の発表、成果の展開等)

適宜メンバーを加えるなどして研究体制は整えられている。研究成果の発表者に偏りが見られるが、チーム全体としてはほぼ計画通りの研究成果だと認められる。

内容は専門的なので、その効果を一般に分かり易く説明することが望ましい。